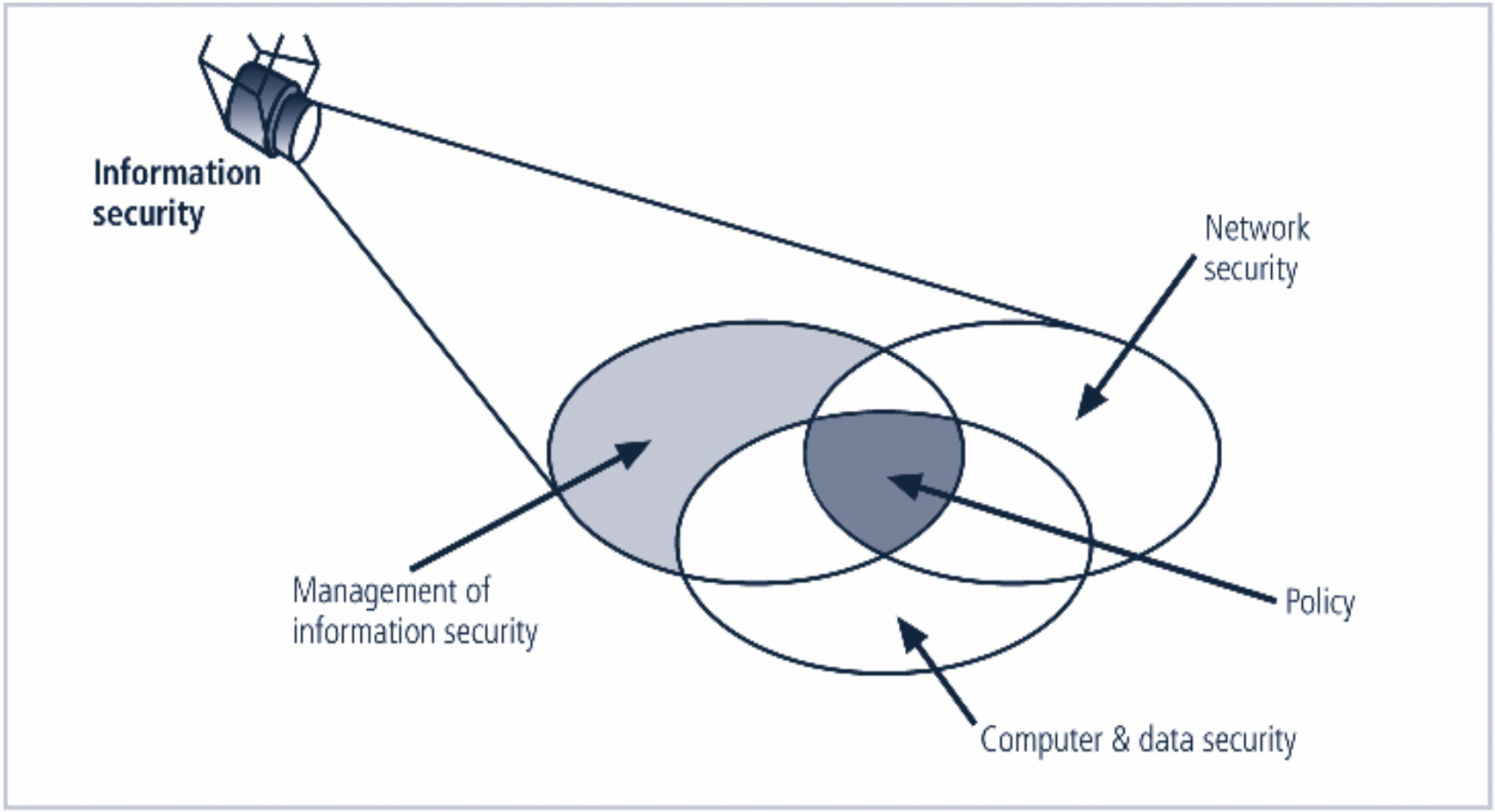
Introduction to Information Security

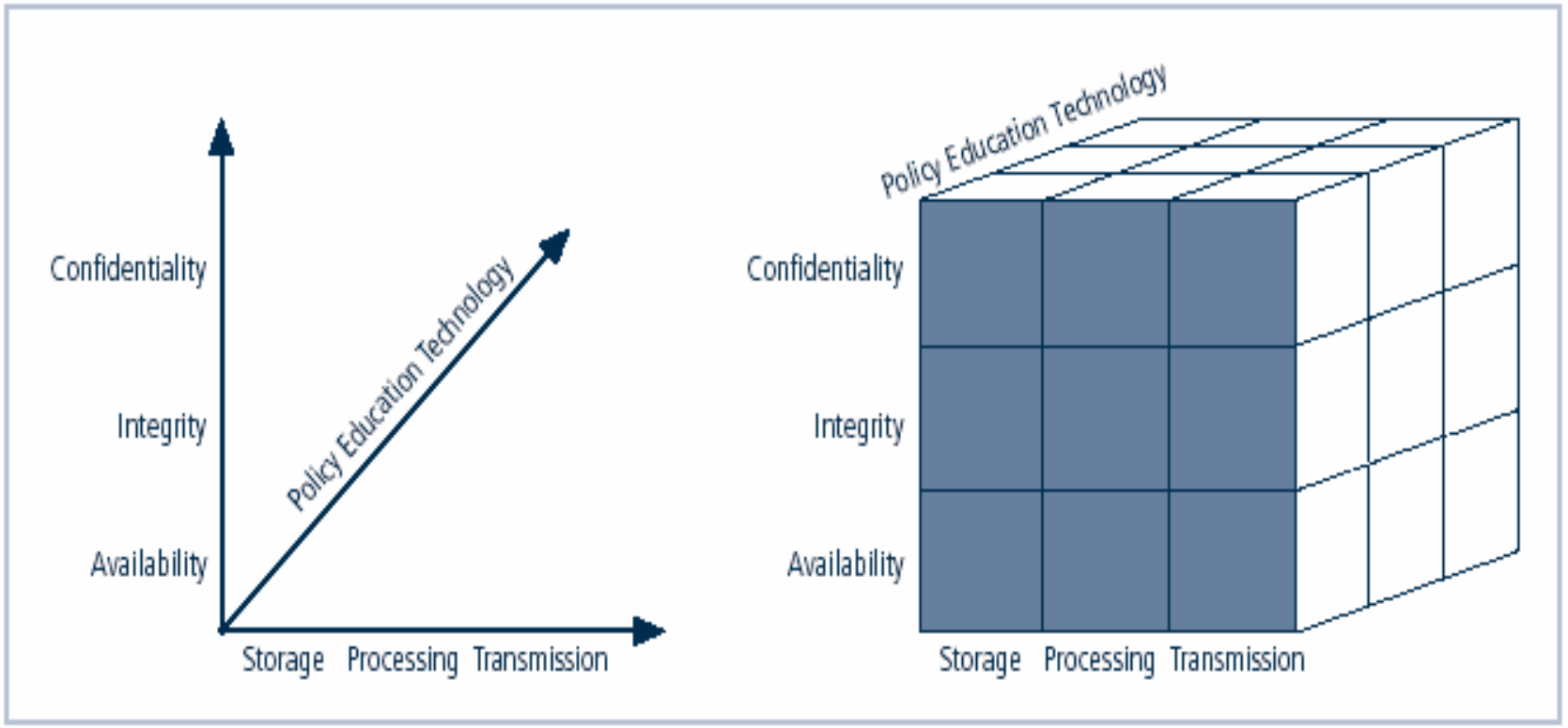
What is Security?

- “The quality or state of being secure—to be free from danger”
- A successful organization should have multiple layers of security in place:
  - Physical security
  - Personal security
  - Operations security
  - Communications security
  - Network security
  - Information security

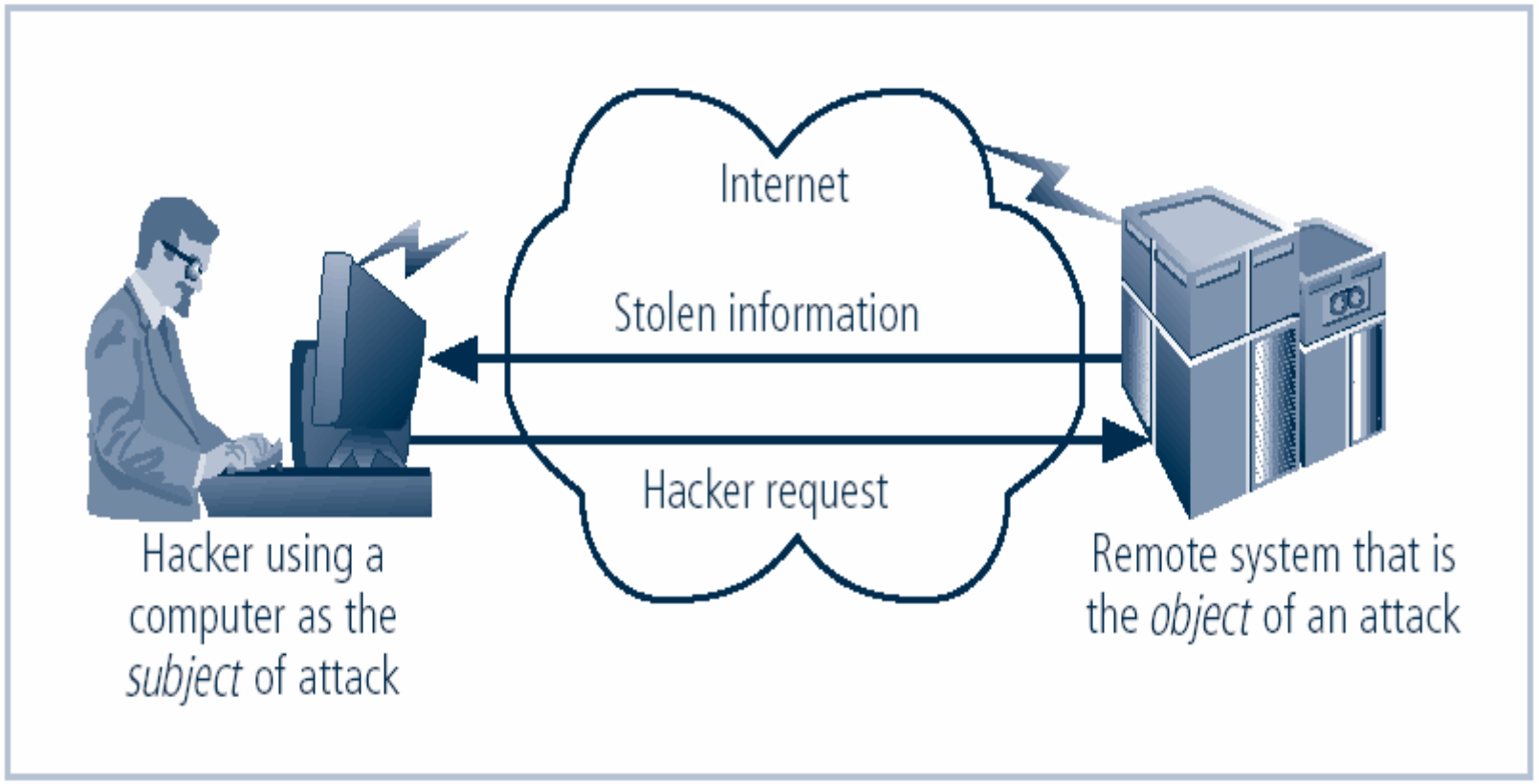


Components of Information Security

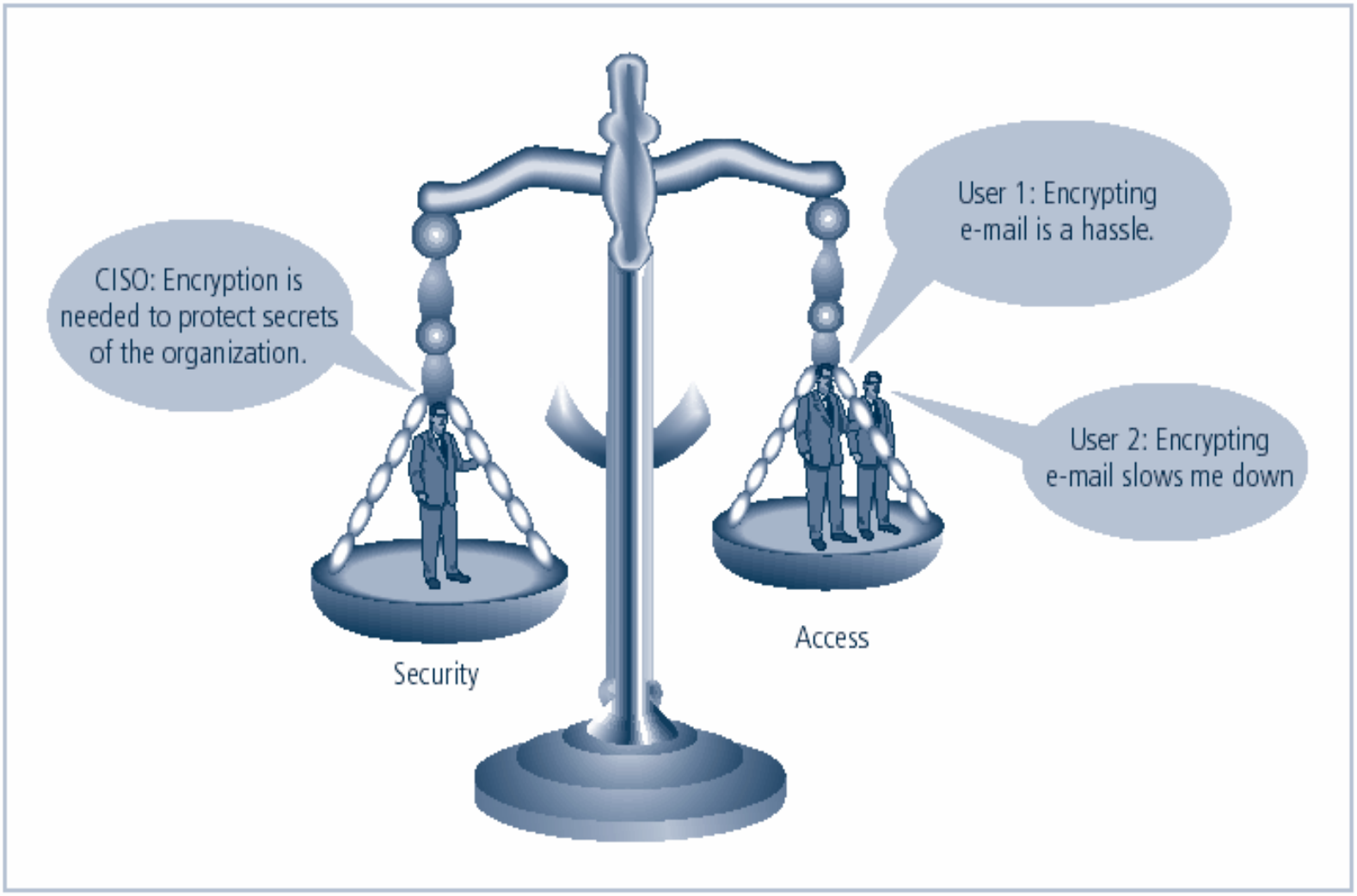
NSTISSC Security Model



NSTISSC Security Model



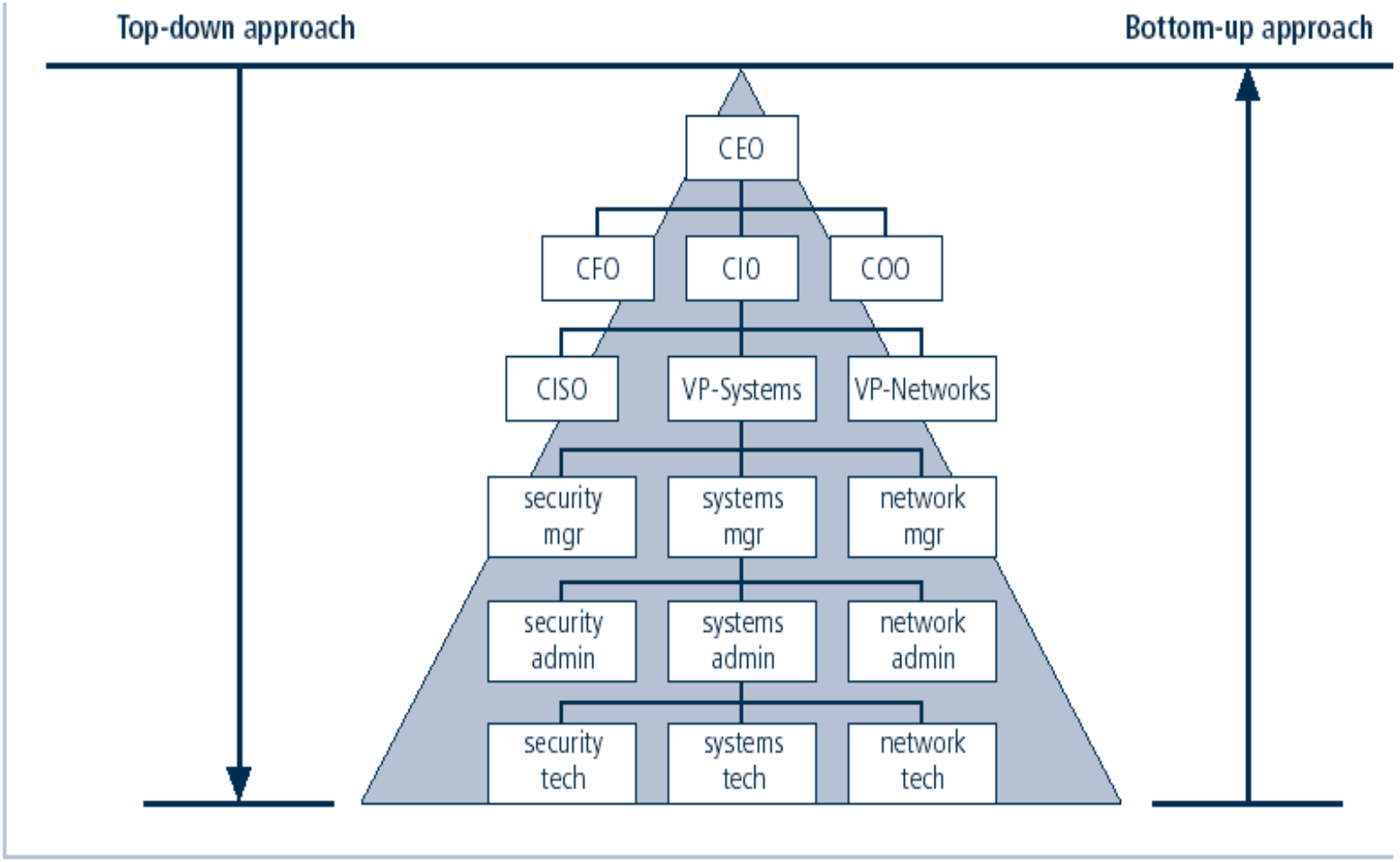
Computer as the Subject and Object of an Attack



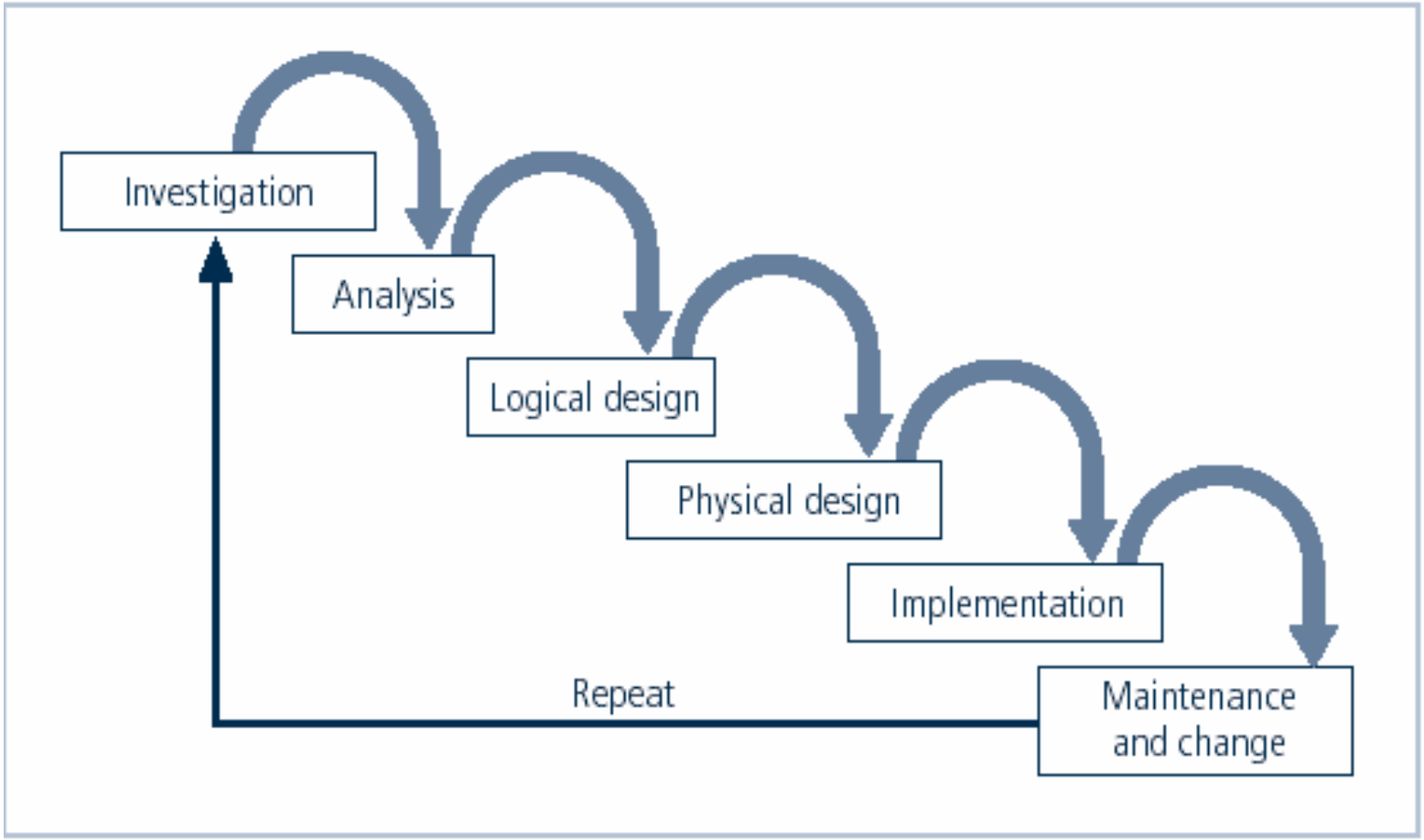
Balancing Information Security and Access

Approaches to Information Security Implementation: Bottom-Up Approach

- Grassroots effort: systems administrators attempt to improve security of their systems
- Key advantage: technical expertise of individual administrators
- Seldom works, as it lacks a number of critical features:
  - Participant support
  - Organizational staying power



Approaches to Information Security Implementation



SDLC Waterfall Methodology

Investigation

- What problem is the system being developed to solve?
- Objectives, constraints and scope of project are specified
- Preliminary cost-benefit analysis is developed
- At the end, feasibility analysis is performed to assesses economic, technical, and behavioral feasibilities of the process

Analysis

- Documents from investigation phase are studied
- Analyzes existing security policies or programs, along with documented current threats and associated controls
- Includes analysis of relevant legal issues that could impact design of the security solution
- The risk management task begins

Logical Design

- Creates and develops blueprints for information security
- Incident response actions planned:
  - Continuity planning
  - Incident response
  - Disaster recovery
- Feasibility analysis to determine whether project should continue or be outsourced

Security Management

- Chief Information Officer (CIO)
  - Senior technology officer
  - Primarily responsible for advising senior executives on strategic planning
- Chief Information Security Officer (CISO)
  - Primarily responsible for assessment, management, and implementation of IS in the organization
  - Usually reports directly to the CIO

Information Security Project Team

- A number of individuals who are experienced in one or more facets of technical and non-technical areas:
  - Champion
  - Team leader
  - Security policy developers
  - Risk assessment specialists
  - Security professionals
  - Systems administrators
  - End users